STRONGLY REGULAR GRAPHS FROM UNIONS OF CYCLOTOMIC CLASSES

TAO FENG*, QING XIANG†

Abstract. We give two constructions of strongly regular Cayley graphs on finite fields $\mathbb{F}_q$ by using union of cyclotomic classes and index 2 Gauss sums. In particular, we obtain twelve infinite families of strongly regular graphs with new parameters.

1. Introduction

All graphs considered in this paper are simple and undirected. A *strongly regular graph srg* (v, k, λ, μ) is a graph with v vertices that is not complete or edgeless and that has the following properties:

(1) Each vertex is adjacent to k vertices, i.e., the graph is regular of valency k,
(2) For any two adjacent vertices x, y, there are exactly λ vertices adjacent to both x and y.
(3) For any two nonadjacent vertices x, y, there are exactly μ vertices adjacent to both x and y.

Classical examples of strongly regular graphs include the Paley graphs. Let $q = 4t+1$ be a prime power. The *Paley graph* Paley(q) is the graph with the finite field $\mathbb{F}_q$ as vertex set, where two vertices are adjacent when they differ by a nonzero square. One can check that Paley(q) is an srg $(4t+1, 2t, t-1, t)$. For a survey on strongly regular graphs, we refer the reader to the lecture notes by Brouwer and Haemers [3]; see also [8]. Strongly regular graphs are also closely related to two-weight codes, two-intersection sets in finite geometry, and partial difference sets. For these connections, we refer the reader to [5, 14]. Let Γ be a graph. The adjacency matrix of Γ is the $(0, 1)$-matrix A indexed by the vertex set $V\Gamma$ of Γ, where $A_{xy} = 1$ when there is an edge between x and y in Γ and $A_{xy} = 0$ otherwise. A useful way to check whether a graph is strongly regular is by using the eigenvalues of its adjacency matrix. For convenience we call an eigenvalue *restricted* if it has an eigenvector perpendicular to the all-ones vector $\mathbf{1}$.

Key words and phrases. Cyclotomy, Gauss sum, index 2 Gauss sum, strongly regular graph, uniform cyclotomy.

*Supported in part by the Fundamental Research Funds for the central universities.

†Research supported in part by NSF Grant DMS 1001557, and by the Overseas Cooperation Fund (grant 10928101) of China.

Theorem 1.1. *For a graph Γ of order v, not complete or edgeless, with adjacency matrix A, the following are equivalent:*

1. *Γ is an srg (v, k, λ, μ) for certain integers k, λ, μ,*
2. *$A^2 = (\lambda - \mu)A + (k - \mu)I + \mu J$ for certain real numbers k, λ, μ, where I, J are the identity matrix and the all-ones matrix, respectively,*
3. *A has precisely two distinct restricted eigenvalues.*

This is Theorem 9.1.2 in [3, p. 115]. The Paley graphs are probably the simplest examples of the so-called cyclotomic strongly regular graphs, which we define below. Let p be a prime, and f be a positive integer. Let $\mathbb{F}_{p^f}$ be the finite field of order p^f, $D \subset \mathbb{F}_{p^f}$ be such that $-D = D$ and $0 \notin D$. We consider the graph Γ with the elements of $\mathbb{F}_{p^f}$ as vertices; two vertices are adjacent if and only if their difference belongs to D. That is, Γ is the Cayley graph on $\mathbb{F}_{p^f}$ with "connection" set D, usually written as $\mathrm{Cay}(\mathbb{F}_{p^f}, D)$. When D is a subgroup of the multiplicative group $\mathbb{F}_{p^f}^*$ of $\mathbb{F}_{p^f}$, and if $\Gamma = \mathrm{Cay}(\mathbb{F}_{p^f}, D)$ is strongly regular, then we speak of a *cyclotomic strongly regular graph.* The problem of classifying all cyclotomic strongly regular graphs is a venerable one. We refer the reader to [16, 12, 18] for detailed studies of this problem. In particular, Schmidt and White [18] proposed a conjectural classification of all cyclotomic srg. In this paper, we are interested in constructing srg $\mathrm{Cay}(\mathbb{F}_{p^f}, D)$, in which D is a union of at least two cosets of a subgroup of $\mathbb{F}_{p^f}^*$ (while a single coset does not give rise to an srg). There are some known examples of such srg. To describe these examples, we fix a primitive element γ of $\mathbb{F}_{p^f}$; let N be an integer greater than 1 such that $N|(p^f - 1)$, C_0 be the subgroup of $\mathbb{F}_{p^f}^*$ of index N, and $C_i = \gamma^i C_0$, $1 \le i \le N - 1$.

Example 1.2. (De Lange, [13]) *Let $p = 2$, $f = 12$, $N = 45$. Then* $\mathrm{Cay}(\mathbb{F}_{p^f}, C_0 \cup C_5 \cup C_{10})$ *is an srg, while* $\mathrm{Cay}(\mathbb{F}_{p^f}, C_0)$ *is not.*

Example 1.3. (Ikuta and Munemasa, [9]) *Let $p = 2$, $f = 20$, $N = 75$. Then* $\mathrm{Cay}(\mathbb{F}_{p^f}, C_0 \cup C_3 \cup C_6 \cup C_9 \cup C_{12})$ *is an srg, while* $\mathrm{Cay}(\mathbb{F}_{p^f}, C_0)$ *is not.*

Example 1.4. (Ikuta and Munemasa, [9]) *Let $p = 2$, $f = 21$, $N = 49$. Then* $\mathrm{Cay}(\mathbb{F}_{p^f}, C_0 \cup C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5 \cup C_6)$ *is an srg, while* $\mathrm{Cay}(\mathbb{F}_{p^f}, C_0)$ *is not.*

We will generalize each of the above three examples into an infinite family. Moreover we obtain nine more infinite families of srg with new parameters by using union of cyclotomic classes.

2. Gauss sums

Let p be a prime, f a positive integer, and $q = p^f$. Let ξ_p be a fixed complex primitive pth root of unity and let $\mathrm{Tr}_{q/p}$ be the trace from $\mathbb{F}_q$ to $\mathbb{Z}/p\mathbb{Z}$. Define

$$\psi : \mathbb{F}_q \to \mathbb{C}^*, \quad \psi(x) = \xi_p^{\mathrm{Tr}_{q/p}(x)}, \tag{2.1}$$

which is easily seen to be a nontrivial character of the additive group of $\mathbb{F}_q$. Let

$$\chi : \mathbb{F}_q^* \to \mathbb{C}^*$$

be a character of $\mathbb{F}_q^*$. We define the *Gauss sum* by

$$g(\chi) = \sum_{a\in\mathbb{F}_q^*} \chi(a)\psi(a).$$

Note that if χ_0 is the trivial multiplicative character of $\mathbb{F}_q$, then $g(\chi_0) = -1$. We are usually concerned with nontrivial Gauss sums $g(\chi)$, i.e., those with $\chi \neq \chi_0$. Gauss sums can be viewed as the Fourier coefficients in the Fourier expansion of $\psi|_{\mathbb{F}_q^*}$ in terms of the multiplicative characters of $\mathbb{F}_q$. That is, for every $c \in \mathbb{F}_q^*$,

$$\psi(c) = \frac{1}{q-1} \sum_{\chi\in\widehat{\mathbb{F}}_q^*} g(\bar{\chi})\chi(c), \tag{2.2}$$

where $\bar{\chi} = \chi^{-1}$ and $\widehat{\mathbb{F}}_q^*$ denotes the character group of $\mathbb{F}_q^*$.

While it is easy to show that the absolute value of a nontrivial Gauss sum $g(\chi)$ is equal to $\sqrt{q}$, the explicit determination of Gauss sums is a difficult problem. However, there are a few cases where the Gauss sums $g(\chi)$ can be explicitly evaluated. The simplest case is the so-called *semi-primitive case*, where there exists an integer j such that $p^j \equiv -1 \pmod N$ and N is the order of χ in $\widehat{\mathbb{F}}_q^*$. Some authors [1, 2] also refer to this case as uniform cyclotomy, or pure Gauss sums. For future use, we state the following theorem dealing with the semi-primitive case.

Theorem 2.1. ([2, p. 364]) *Let p be a prime, and $N > 2$ be an integer. Suppose that there is a positive integer t such that $p^t \equiv -1$ (mod N), with t chosen minimal. Let χ be a character of order N of $\mathbb{F}_{p^r}^*$ for some positive integer r. Then $r = 2ts$ for some positive integer s, and*

$$p^{-r/2}g(\chi) = \begin{cases} (-1)^{s-1}, & \text{if } p = 2,\\ (-1)^{s-1+\frac{(p^t+1)s}{N}}, & \text{if } p > 2. \end{cases}$$

The next interesting case is the index 2 case, where -1 is not in the subgroup $\langle p\rangle$, the cyclic group generated by p (the characteristic of the finite field $\mathbb{F}_q$), and $\langle p\rangle$ has index 2 in $(\mathbb{Z}/N\mathbb{Z})^*$ (again here N is the order of χ in $\widehat{\mathbb{F}}_q^*$). Many authors have studied this case, including McEliece [16], Langevin [11], Mbodj [15], Meijer and Van der Vlugt [17], and Yang and Xia [19]. We state here some results in the index 2 case which will be used in our constructions of strongly regular graphs. Below we use $\phi(N)$ to denote the number of integers k with $1 \le k \le N$ such that $\gcd(k, N) = 1$, and $\mathrm{ord}_N(p)$ to denote the order of p modulo N, which is the smallest positive integer f such that $p^f \equiv 1 \pmod N$.

Theorem 2.2. (Langevin [11]) *Let $N = p_1^m$, where m is a positive integer, p_1 is a prime such that $p_1 > 3$ and $p_1 \equiv 3$ (mod 4). Let p be a prime such* *that* $[(\mathbb{Z}/N\mathbb{Z})^* : \langle p\rangle] = 2$ *(that is,* $f := \mathrm{ord}_N(p) = \phi(N)/2$*) and let* $q = p^f$*. Let* χ *be a multiplicative character of order* N *of* $\mathbb{F}_q$*, and* h *be the class number of* $\mathbb{Q}(\sqrt{-p_1})$*. Then the Gauss sum* $g(\chi)$ *over* $\mathbb{F}_q$ *is determined up to complex conjugation by*

$$g(\chi) = \frac{b + c\sqrt{-p_1}}{2} p^{h_0},$$

where

1. $h_0 = \frac{f-h}{2}$,
2. $b, c \not\equiv 0$ *(mod* p*),*
3. $b^2 + p_1 c^2 = 4p^h$,
4. $bp^{h_0} \equiv -2$ *(mod* p_1*).*

Theorem 2.3. (Mbodj [15]) *Let* $N = p_1^m p_2^n$*, where* m, n *are positive integers,* p_1 *and* p_2 *are primes such that* $\{p_1 \pmod 4, p_2 \pmod 4\} = \{1, 3\}$, $\mathrm{ord}_{p_1^m}(p) = \phi(p_1^m)$, $\mathrm{ord}_{p_2^n}(p) = \phi(p_2^n)$*. Let* p *be a prime such that* $[(\mathbb{Z}/N\mathbb{Z})^* : \langle p\rangle] = 2$ *(that is,* $f := \mathrm{ord}_N(p) = \phi(N)/2$*) and let* $q = p^f$*. Let* χ *be a multiplicative character of order* N *of* $\mathbb{F}_q$*, and* h *be the class number of* $\mathbb{Q}(\sqrt{-p_1p_2})$*. Then the Gauss sum* $g(\chi)$ *over* $\mathbb{F}_q$ *is determined up to complex conjugation by*

$$g(\chi) = \frac{b + c\sqrt{-p_1p_2}}{2} p^{h_0},$$

where

1. $h_0 = \frac{f-h}{2}$,
2. $b, c \not\equiv 0$ *(mod* p*),*
3. $b^2 + p_1p_2c^2 = 4p^h$,
4. $b \equiv 2p^{h/2}$ *(mod* ℓ*), here* $\ell \in \{p_1, p_2\}$ *is the prime congruent to 3 modulo 4.*

3. Cyclotomic classes and periods

Let $q = p^f$ be a prime power, and let γ be a fixed primitive element of $\mathbb{F}_q$. Let $N > 1$ be a divisor of $q - 1$. We define the N-th *cyclotomic classes* $C_0, C_1, \dots, C_{N-1}$ by

$$C_i = \{\gamma^{jN+i} \mid 0 \le j \le \frac{q-1}{N} - 1\},$$

where $0 \le i \le N - 1$. That is, C_0 is the subgroup of $\mathbb{F}_q^*$ consisting of all nonzero N-th powers in $\mathbb{F}_q$, and $C_i = \gamma^i C_0$, $1 \le i \le N - 1$.

Let ψ be the additive character of $\mathbb{F}_q$ defined in (2.1). The N-th *cyclotomic periods* are defined by

$$\eta_a = \sum_{x \in C_a} \psi(x),$$

where $0 \le a \le N-1$. The relationship between Gauss sums and cyclotomic periods are given as follows. Using (2.2), we have

$$\begin{aligned}
\eta_a &= \sum_{x\in C_0} \psi(\gamma^a x)\\
&= \sum_{x\in C_0} \frac{1}{q-1} \sum_{\chi\in\widehat{\mathbb{F}_q^*}} g(\bar{\chi})\chi(\gamma^a x)\\
&= \frac{1}{(q-1)} \sum_{\chi\in\widehat{\mathbb{F}_q^*}} g(\bar{\chi})\chi(\gamma^a) \sum_{x\in C_0} \chi(x)\\
&= \frac{1}{N} \sum_{\chi\in C_0^\perp} g(\bar{\chi})\chi(\gamma^a)
\end{aligned}$$

where $C_0^\perp$ is the subgroup of $\widehat{\mathbb{F}_q^*}$ consisting of all χ which are trivial on C_0, i.e., $C_0^\perp$ is the unique subgroup of order N. This shows that cyclotomic periods (multiplied by N) are linear combinations of Gauss sums with coefficients being complex N-th roots of unity.

As we already mentioned in Section 2, the case when $\mathrm{ord}_N(p) = \phi(N)/2$ and $-1 \notin \langle p\rangle \le \mathbb{Z}_N^*$ is usually called *the index 2 case*. It is an easy exercise to show that in the index 2 case, N has at most two odd prime divisors. Assume that N is odd, we have the following three possibilities in the index 2 case (see [19]). Below both p_1 and p_2 are prime.

(1) $N = p_1^m$, $p_1 \equiv 3 \pmod 4$;
(2) $N = p_1^m p_2^n$, $\{p_1 \pmod 4, p_2 \pmod 4\} = \{1,3\}$, $\mathrm{ord}_{p_1^m}(p) = \phi(p_1^m)$, $\mathrm{ord}_{p_2^n}(p) = \phi(p_2^n)$;
(3) $N = p_1^m p_2^n$, $p_1 \equiv 1, 3 \pmod 4$, $\mathrm{ord}_{p_1^m}(p) = \phi(p_1^m)$ and $p_2 \equiv 3 \pmod 4$, $\mathrm{ord}_{p_2^n}(p) = \phi(p_2^n)/2$.

In the following two sections we will consider the cases where new strongly regular graphs are constructed by taking union of cyclotomic classes.

4. The index 2 case with $N = p_1^m$

In this section we assume that $N = p_1^m$ (here $m \ge 1$, $p_1 > 3$ is a prime such that $p_1 \equiv 3 \pmod 4$), p is a prime such that $\gcd(N, p) = 1$, and $f := \mathrm{ord}_N(p) = \phi(N)/2$. Let $q = p^f$, and as before let $C_0, C_1, \ldots, C_{N-1}$ be the N-th cyclotomic classes of $\mathbb{F}_q$. Note that $-C_i = C_i$ for all $0 \le i \le N-1$ since either $2N|(q-1)$ or q is even. Define

$$D = \bigcup_{i=0}^{p_1^{m-1}-1} C_i \tag{4.1}$$

Using D as connection set, we construct the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$.

Theorem 4.1. *The Cayley graph* $\mathrm{Cay}(\mathbb{F}_q, D)$ *is a regular graph of valency* $|D|$*, and it has at most three distinct restricted eigenvalues.*

Proof: Since $-D = D$ and $0 \notin D$, the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$ is undirected and without loops. It is also regular of valency $|D|$. The restricted eigenvalues of this Cayley graph, as explained in [4] (see also [3, p. 134]), are

$$\psi(\gamma^a D) := \sum_{x \in D} \psi(\gamma^a x),$$

where γ is a fixed primitive element of $\mathbb{F}_q$, ψ is the additive character of $\mathbb{F}_q$ defined in (2.1) and $0 \leq a \leq N-1$.

We have

$$\begin{aligned} \psi(\gamma^a D) &= \sum_{i=0}^{p_1^{m-1}-1} \psi(\gamma^a C_i) \\ &= \sum_{i=0}^{p_1^{m-1}-1} \eta_{a+i} \\ &= \frac{1}{N} \sum_{\chi \in C_0^\perp} g(\bar{\chi}) \sum_{i=0}^{p_1^{m-1}-1} \chi(\gamma^{a+i}), \end{aligned}$$

where $C_0^\perp$ is the unique subgroup of $\widehat{\mathbb{F}}_q^*$ of order $N = p_1^m$. For convenience we define

$$T_a = \sum_{\chi \in C_0^\perp} g(\bar{\chi}) \sum_{i=0}^{p_1^{m-1}-1} \chi(\gamma^{a+i}).$$

If $\chi \in C_0^\perp$ and $o(\chi) = 1$, then $g(\bar{\chi}) = -1$, and $\sum_{i=0}^{p_1^{m-1}-1} \chi(\gamma^{a+i}) = p_1^{m-1}$. If $\chi \in C_0^\perp$ and $o(\chi) = p_1^i$ $(1 \leq i \leq m-1)$, then $\sum_{i=0}^{p_1^{m-1}-1} \chi(\gamma^{a+i}) = \chi(\gamma^a)\frac{\chi(\gamma)^{p_1^{m-1}}-1}{\chi(\gamma)-1} = 0$. Therefore we have

$$T_a = -p_1^{m-1} + \sum_{t \in \mathbb{Z}_{p_1^m}^*} g(\bar{\chi}^t) \sum_{i=0}^{p_1^{m-1}-1} \chi^t(\gamma^{a+i}),$$

where χ is the character of $\mathbb{F}_q^*$ defined by

$$\chi(\gamma) = \exp(\frac{2\pi i}{N}). \tag{4.2}$$

By Theorem 2.2, we have

$$g(\bar{\chi}) = \frac{b + c\sqrt{-p_1}}{2} p^{h_0}, \quad b, c \not\equiv 0 \pmod{p},$$

where $h_0 = \frac{f-h}{2}$ and h is the class number of $\mathbb{Q}(\sqrt{-p_1})$, $b^2 + p_1 c^2 = 4p^h$, and $bp^{h_0} \equiv -2 \pmod{p_1}$. It follows that for any $t \in \mathbb{Z}_{p_1^m}^*$, $g(\bar{\chi}^t) =$

$\frac{b+c(\frac{t}{p_1})\sqrt{-p_1}}{2}p^{h_0}$, where $(\frac{\cdot}{p_1})$ is the Lengdre symbol.

For each a, $0 \leq a \leq N-1$, there is a unique $i_a \in \{0, 1, \dots, p_1^{m-1}-1\}$, such that $p_1^{m-1}|(a+i_a)$. Write $a + i_a = p_1^{m-1}j_a$ (e.g., when $N = p_1$, we simply have $j_a = a$). For convenience, we introduce the Kronecker delta δ_{j_a}, which equals 1 if $p_1|j_a$, and 0 otherwise. For each $t \in \mathbb{Z}^*_{p_1^m}$, we write $t = t_1 + p_1 t_2$, where $t_1 \in \mathbb{Z}^*_{p_1}$ and $t_2 \in \mathbb{Z}_{p_1^{m-1}}$. Now we can compute

$$\begin{aligned}
T_a + p_1^{m-1} =& \sum_{t \in \mathbb{Z}^*_{p_1^m}} g(\bar{\chi}^t) \sum_{i=0}^{p_1^{m-1}-1} \chi^t(\gamma^{a+i}) \\
=& p^{h_0} \sum_{t_1 \in \mathbb{Z}^*_{p_1}} \sum_{i=0}^{p_1^{m-1}-1} \chi^{t_1}(\gamma^{a+i}) \frac{b + c(\frac{t_1}{p_1})\sqrt{-p_1}}{2} \sum_{t_2 \in \mathbb{Z}_{p_1^{m-1}}} \chi^{p_1 t_2}(\gamma^{a+i}) \\
=& p^{h_0} p_1^{m-1} \sum_{t_1 \in \mathbb{Z}^*_{p_1}} \chi^{p_1^{m-1}t_1}(\gamma^{j_a}) \frac{b + c(\frac{t_1}{p_1})\sqrt{-p_1}}{2} \\
=& \frac{p^{h_0} p_1^{m-1} b}{2} \sum_{t_1 \in \mathbb{Z}^*_{p_1}} \chi^{p_1^{m-1}t_1}(\gamma^{j_a}) + \frac{p^{h_0} p_1^{m-1} c\sqrt{-p_1}}{2} \sum_{t_1 \in \mathbb{Z}^*_{p_1}} \chi^{p_1^{m-1}t_1}(\gamma^{j_a}) \left(\frac{t_1}{p_1}\right) \\
=& \frac{p^{h_0} p_1^{m-1} b}{2}(p_1\delta_{j_a} - 1) + \frac{p^{h_0} p_1^{m-1} c\sqrt{-p_1}}{2} \left(\frac{j_a}{p_1}\right)\sqrt{-p_1} \\
=& \frac{p^{h_0} p_1^{m-1} b}{2}(p_1\delta_{j_a} - 1) - \frac{p^{h_0} p_1^{m} c}{2} \left(\frac{j_a}{p_1}\right).
\end{aligned}$$

We remark that when $N = p_1$ (i.e., $m = 1$), the second line in the above computations needs to be deleted; everything else still holds true in this case. Therefore we have

$$T_a + p_1^{m-1} = \begin{cases} \frac{p^{h_0}p_1^m b}{2} - \frac{p^{h_0}p_1^{m-1} b}{2}, & \text{if } (\frac{j_a}{p_1}) = 0, \\ \pm\frac{p^{h_0}p_1^m c}{2} - \frac{p^{h_0}p_1^{m-1} b}{2}, & \text{if } (\frac{j_a}{p_1}) \neq 0. \end{cases}$$

The eigenvalues of $\mathrm{Cay}(\mathbb{F}_q, D)$ are $|D| = p_1^{m-1}\frac{q-1}{N} = \frac{p^f-1}{p_1}$, and

$$\psi(\gamma^a D) = \frac{1}{N}T_a = \begin{cases} \frac{p^{h_0}b}{2} - \frac{p^{h_0}b}{2p_1} - \frac{1}{p_1}, & \text{if } (\frac{j_a}{p_1}) = 0, \\ \pm\frac{p^{h_0}c}{2} - \frac{p^{h_0}b}{2p_1} - \frac{1}{p_1}, & \text{if } (\frac{j_a}{p_1}) \neq 0, \end{cases}$$

where $0 \leq a \leq N-1$. So $\mathrm{Cay}(\mathbb{F}_q, D)$ has at most three distinct restricted eigenvalues. The proof is now complete. □

Let χ be the multiplicative character defined in (4.2), and let

$$g(\bar{\chi}) = \frac{b + c\sqrt{-p_1}}{2}p^{h_0}, \quad b, c \not\equiv 0 \pmod{p}, \tag{4.3}$$

where $h_0 = \frac{f-h}{2}$ and h is the class number of $\mathbb{Q}(\sqrt{-p_1})$, $b^2 + p_1c^2 = 4p^h$, and $bp^{h_0} \equiv -2 \pmod{p_1}$. We note that while c can only be determined up to sign, b is uniquely determined (without sign ambiguity) by the condition that $bp^{h_0} \equiv -2 \pmod{p_1}$. We have the following corollary.

Corollary 4.2. *Using the above notation,* $\mathrm{Cay}(\mathbb{F}_q, D)$ *is a strongly regular graph if and only if* $b, c \in \{1, -1\}$.

Proof: If $\mathrm{Cay}(\mathbb{F}_q, D)$ is a strongly regular graph, then by Theorem 1.1 it has precisely two distinct restricted eigenvalues, r and s. As usual, we use r to denote the positive eigenvalue, and s the negative one. By Theorem 4.1 and the explicit computations of eigenvalues in its proof, we must have $c = \pm b$. Since $\gcd(b, c)$ divides $4p^h$ and $b, c \not\equiv 0 \pmod{p}$, the condition that $c = \pm b$ is equivalent to $b, c \in \{1, -1\}$ or $b, c \in \{2, -2\}$. It is impossible to have $b, c \in \{2, -2\}$: otherwise, from $1 + p_1 = p^h$ we deduce that $p = 2$, contradicting the fact $b, c \not\equiv 0 \pmod{p}$. Therefore we conclude that $b, c \in \{1, -1\}$.

Fo the converse, noting that if $b, c \in \{1, -1\}$, then $\psi(\gamma^a D)$, $0 \leq a \leq N-1$, take only two distinct values. Hence $\mathrm{Cay}(\mathbb{F}_q, D)$ has precisely two distinct restricted eigenvalues. By Theorem 1.1, $\mathrm{Cay}(\mathbb{F}_q, D)$ is strongly regular. The proof is now complete. □

Now if $N = p_1^m$, p_1 is a prime congruent to 3 modulo 4, $p_1 > 3$, and $\frac{1+p_1}{4} = p^h$ for some prime p, where h is the class number of $\mathbb{Q}(\sqrt{-p_1})$, and $f := \mathrm{ord}_N(p) = \phi(N)/2$, then the only possible b, c satisfying (4.3) must be ± 1. This can be seen as follows: from $b^2 + p_1c^2 = 4p^h = 1 + p_1$ and $b, c \not\equiv 0 \pmod{p}$, we get that $1 + p_1 \leq b^2 + p_1c^2 = 1 + p_1$, hence $b, c \in \{1, -1\}$. Therefore by Corollary 4.2, under the above assumptions, the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$ is strongly regular. Also we note that under the above assumptions, we can further determine when b is equal to 1 and when b is equal to -1: First of all, we note that since $[\mathbb{Z}^*_{p_1^m} : \langle p \rangle] = 2$, we have $(\frac{p}{p_1}) = 1$. When $p_1 \equiv 3 \pmod{8}$, we have $(\frac{2}{p_1}) = -1$; raising both sides of $p^{h_0}b \equiv -2 \pmod{p_1}$ to the $\frac{p_1-1}{2}$th power, we obtain $b(\frac{p}{p_1})^{h_0} = (\frac{-1}{p_1})(\frac{2}{p_1}) = 1$, from which we get $b = 1$. Similarly, when $p_1 \equiv 7 \pmod{8}$, we get $b = -1$. We now set out to find explicit examples of strongly regular Cayley graphs in this way. In the following we only list the examples with $m \geq 2$ since the $m = 1$ case was considered previously by Langevin in [12]; see also [18].

Example 4.3. Let $p = 2$, $p_1 = 7$, $N = p_1^m$, $m \geq 2$ is an integer. It is straightforward to check that $\mathrm{ord}_{7^2}(2) = 21 = \phi(7^2)/2$. One can easily prove by induction that $\mathrm{ord}_N(2) = \phi(7^m)/2$ for all $m \geq 2$. The class number h of $\mathbb{Q}(\sqrt{-7})$ is equal to 1 (c.f. [6, p. 514]). Therefore we indeed have $\frac{1+p_1}{4} = p^h$ in this case. We have $f = 3 \cdot 7^{m-1}$, $b = -1$, $h_0 = \frac{f-1}{2}$. Therefore we obtain a strongly regular Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$, with $v = q = 2^{3 \cdot 7^{m-1}}$, $k = \frac{v-1}{7}$, and with restricted eigenvalues $r = \frac{2^{h_0+2}-1}{7}$, $s = \frac{-3 \cdot 2^{h_0}-1}{7}$.

We remark that when $m = 2$, the srg in Example 4.3 is the same as $\mathrm{Cay}(\mathbb{F}_{2^{21}}, R_1)$ in Example 3 of [9].

Example 4.4. Let $p = 3$, $p_1 = 107$, $N = p_1^m$, $m \geq 2$ is an integer. It is straightforward to check that $\mathrm{ord}_{107^2}(3) = 5671 = \phi(107^2)/2$. One can easily prove by induction that $\mathrm{ord}_N(3) = \phi(107^m)/2$ for all $m \geq 2$. The class number h of $\mathbb{Q}(\sqrt{-107})$ is equal to 3 (c.f. [6, p. 514]). Therefore we indeed have $\frac{1+p_1}{4} = p^h$ in this case. We have $f = 53 \cdot 107^{m-1}$, $b = 1$, $h_0 = \frac{f-3}{2}$. Therefore we obtain a strongly regular Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$, with $v = q = 3^{53 \cdot 107^{m-1}}$, $k = \frac{v-1}{107}$, and with restricted eigenvalues $r = \frac{53 \cdot 3^{h_0} - 1}{107}$, $s = \frac{-54 \cdot 3^{h_0} - 1}{107}$.

Example 4.5. Let $p = 5$, $p_1 = 19$, $N = p_1^m$, $m \geq 2$ is an integer. It is straightforward to check that $\mathrm{ord}_{19^2}(5) = 171 = \phi(19^2)/2$. One can easily prove by induction that $\mathrm{ord}_N(5) = \phi(19^m)/2$ for all $m \geq 2$. The class number h of $\mathbb{Q}(\sqrt{-19})$ is equal to 1 (c.f. [6, p. 514]). Therefore we indeed have $\frac{1+p_1}{4} = p^h$ in this case. We have $f = 9 \cdot 19^{m-1}$, $b = 1$, $h_0 = \frac{f-1}{2}$. Therefore we obtain a strongly regular Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$, with $v = q = 5^{9 \cdot 19^{m-1}}$, $k = \frac{v-1}{19}$, and with restricted eigenvalues $r = \frac{9 \cdot 5^{h_0} - 1}{19}$, $s = \frac{-10 \cdot 5^{h_0} - 1}{19}$.

Example 4.6. Let $p = 5$, $p_1 = 499$, $N = p_1^m$, $m \geq 2$ is an integer. It is straightforward to check that $\mathrm{ord}_{499^2}(5) = 124251 = \phi(499^2)/2$. One can easily prove by induction that $\mathrm{ord}_N(5) = \phi(499^m)/2$ for all $m \geq 2$. The class number h of $\mathbb{Q}(\sqrt{-499})$ is equal to 3 (c.f. [6, p. 514]). Therefore we indeed have $\frac{1+p_1}{4} = p^h$ in this case. We have $f = 249 \cdot 499^{m-1}$, $b = 1$, $h_0 = \frac{f-3}{2}$. Therefore we obtain a strongly regular Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$, with $v = q = 5^{249 \cdot 499^{m-1}}$, $k = \frac{v-1}{499}$, and with restricted eigenvalues $r = \frac{249 \cdot 5^{h_0} - 1}{499}$, $s = \frac{-250 \cdot 5^{h_0} - 1}{499}$.

Example 4.7. Let $p = 17$, $p_1 = 67$, $N = p_1^m$, $m \geq 2$ is an integer. It is straightforward to check that $\mathrm{ord}_{67^2}(17) = 2211 = \phi(67^2)/2$. One can easily prove by induction that $\mathrm{ord}_N(17) = \phi(67^m)/2$ for all $m \geq 2$. The class number h of $\mathbb{Q}(\sqrt{-67})$ is equal to 1 (c.f. [6, p. 514]). Therefore we indeed have $\frac{1+p_1}{4} = p^h$ in this case. We have $f = 33 \cdot 67^{m-1}$, $b = 1$, $h_0 = \frac{f-1}{2}$. Therefore we obtain a strongly regular Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$, with $v = q = 17^{33 \cdot 67^{m-1}}$, $k = \frac{v-1}{67}$, and with restricted eigenvalues $r = \frac{33 \cdot 67^{h_0} - 1}{67}$, $s = \frac{-34 \cdot 67^{h_0} - 1}{67}$.

Example 4.8. Let $p = 41$, $p_1 = 163$, $N = p_1^m$, $m \geq 2$ is an integer. It is straightforward to check that $\mathrm{ord}_{163^2}(41) = 13203 = \phi(163^2)/2$. One can easily prove by induction that $\mathrm{ord}_N(41) = \phi(163^m)/2$ for all $m \geq 2$. The class number h of $\mathbb{Q}(\sqrt{-163})$ is equal to 1 (c.f. [6, p. 514]). Therefore we indeed have $\frac{1+p_1}{4} = p^h$ in this case. We have $f = 81 \cdot 163^{m-1}$, $b = 1$, $h_0 = \frac{f-1}{2}$. Therefore we obtain a strongly regular Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$, with

$v = q = 41^{81\cdot 163^{m-1}}$, $k = \frac{v-1}{163}$, and with restricted eigenvalues $r = \frac{81\cdot 41^{h_0}-1}{163}$, $s = \frac{-82\cdot 41^{h_0}-1}{163}$.

5. The index 2 case with $N = p_1^m p_2$

In this section, we assume that $N = p_1^m p_2$ $(m \geq 1)$, p_1, p_2 are primes such that $\{p_1 \pmod 4, p_2 \pmod 4\} = \{1, 3\}$, p is a prime such that $\gcd(p, N) = 1$, $\mathrm{ord}_{p_1^m}(p) = \phi(p_1^m)$ and $\mathrm{ord}_{p_2}(p) = \phi(p_2)$, and $f := \mathrm{ord}_N(p) = \phi(N)/2$. Therefore, we are in Case (2), with $n = 1$, as listed in the end of Section 3. Let $q = p^f$, and as before let γ be a fixed primitive element of $\mathbb{F}_q$, $C_0 = \langle \gamma^N \rangle, C_1 = \gamma C_0, \ldots, C_{N-1} = \gamma^{N-1} C_0$ be the N-th cyclotomic classes of $\mathbb{F}_q$. Note that we have $-C_i = C_i$ for all $0 \leq i \leq N-1$ since either $2N|(q-1)$ or q is even. Define

$$D = \bigcup_{i=0}^{p_1^{m-1}-1} C_{ip_2} \tag{5.1}$$

Using D as connection set, we construct the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$.

Theorem 5.1. *The Cayley graph* $\mathrm{Cay}(\mathbb{F}_q, D)$ *is a regular graph of valency* $|D|$*, and it has at most five distinct restricted eigenvalues.*

Proof: Since $-D = D$ and $0 \notin D$, the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$ is undirected and without loops. It is also regular of valency $|D|$. The restricted eigenvalues of this Cayley graph, as explained in [4], are

$$\psi(\gamma^a D) := \sum_{x \in D} \psi(\gamma^a x),$$

where γ is a fixed primitive element of $\mathbb{F}_q$, ψ is the additive character of $\mathbb{F}_q$ defined in (2.1) and $0 \leq a \leq N-1$.

We have

$$\begin{aligned} \psi(\gamma^a D) &= \sum_{i=0}^{p_1^{m-1}-1} \psi(\gamma^a C_{ip_2}) \\ &= \sum_{i=0}^{p_1^{m-1}-1} \eta_{a+ip_2} \\ &= \frac{1}{N} \sum_{\chi \in C_0^\perp} g(\bar{\chi}) \chi(\gamma^a) \sum_{i=0}^{p_1^{m-1}-1} \chi^{p_2}(\gamma^i), \end{aligned}$$

where $C_0^\perp$ is the unique subgroup of $\widehat{\mathbb{F}}_q^*$ of order $N = p_1^m p_2$. For convenience we define

$$T_a = \sum_{\chi \in C_0^\perp} g(\bar{\chi}) \chi(\gamma^a) \sum_{i=0}^{p_1^{m-1}-1} \chi^{p_2}(\gamma^i).$$

If $\chi \in C_0^\perp$, $\chi^{p_2} \neq 1$ and $\chi^{p_1^{m-1}p_2} = 1$, then $\sum_{i=0}^{p_1^{m-1}-1} \chi^{p_2}(\gamma^i) = \frac{\chi^{p_2 p_1^{m-1}}(\gamma)-1}{\chi^{p_2}(\gamma)-1} = 0$. If $\chi \in C_0^\perp$ and $\chi^{p_2} = 1$, then $\sum_{i=0}^{p_1^{m-1}-1} \chi^{p_2}(\gamma^i) = p_1^{m-1}$. Therefore,

$$T_a = p_1^{m-1}(-1 + A) + B + C,$$

where

$$A = \sum_{\substack{\chi \in C_0^\perp \\ o(\chi)=p_2}} g(\bar{\chi})\chi(\gamma^a), \quad B = \sum_{\substack{\chi \in C_0^\perp \\ o(\chi)=p_1^m}} g(\bar{\chi})\chi(\gamma^a) \sum_{i=0}^{p_1^{m-1}-1} \chi^{p_2}(\gamma^i),$$

$$C = \sum_{\substack{\chi \in C_0^\perp \\ o(\chi)=N}} g(\bar{\chi})\chi(\gamma^a) \sum_{i=0}^{p_1^{m-1}-1} \chi^{p_2}(\gamma^i).$$

Below we will compute A, B, C individually.

For each a, $0 \leq a \leq N-1$, there is a unique $i_a \in \{0, 1, \ldots, p_1^{m-1}-1\}$, such that $p_1^{m-1}|(a+p_2 i_a)$. Write $a + p_2 i_a = p_1^{m-1} j_a$. Again we introduce the Kronecker delta δ_{j_a,p_1}, which equals 1 if $p_1|j_a$, 0 otherwise. Also we define δ_{a,p_2} by setting it equal to 1 if $p_2|a$, 0 otherwise.

Since $\mathrm{ord}_{p_2}(p) = \phi(p_2)$, we have $p^{\frac{p_2-1}{2}} \equiv -1 \pmod{p_2}$. By Theorem 2.1, we have $g(\bar{\chi}) = (-1)^{\frac{p_1-1}{2}-1}\sqrt{q}$ for each χ of order p_2. It follows that

$$A = (-1)^{\frac{p_1-1}{2}-1}\sqrt{q} \sum_{o(\chi)=p_2} \chi(\gamma^a) = (-1)^{\frac{p_1-1}{2}-1}\sqrt{q}(p_2\delta_{a,p_2} - 1).$$

Similarly, we have $g(\bar{\chi}) = (-1)^{\frac{p_2-1}{2}-1}\sqrt{q}$ for each χ of order p_1^m. Let χ_1 be the character of order p_1^m in $\widehat{\mathbb{F}}_q^*$ defined by $\chi_1(\gamma) = \exp(\frac{2\pi i}{p_1^m})$. We have

$$B = (-1)^{\frac{p_2-1}{2}-1}\sqrt{q} \sum_{i=0}^{p_1^{m-1}-1} \sum_{t \in \mathbb{Z}_{p_1^m}^*} {\chi_1}^{t(p_2 i + a)}(\gamma) = (-1)^{\frac{p_2-1}{2}-1}\sqrt{q} p_1^{m-1}(p_1\delta_{j_a,p_1} - 1).$$

Let χ_1 be defined as above and χ_2 be the character of order p_2 in $\widehat{\mathbb{F}}_q^*$ defined by $\chi_2(\gamma) = \exp(\frac{2\pi i}{p_2})$. By Theorem 2.3, we have

$$g(\bar{\chi}_1\bar{\chi}_2) = \frac{b + c\sqrt{-p_1p_2}}{2} p^{h_0}, \tag{5.2}$$

where $h_0 = \frac{f-h}{2}$ (h is the class number of $\mathbb{Q}(\sqrt{-p_1p_2})$), $b, c \not\equiv 0 \pmod{p}$, $b^2 + p_1p_2c^2 = 4p^h$, and $b \equiv 2p^{h/2} \pmod{\ell}$, here $\ell \in \{p_1, p_2\}$ is the prime congruent to 3 modulo 4.

Every character in $C_0^\perp$ of order $p_1^m p_2$ is of the form $\chi_1^u\chi_2^v$ with $u \in \mathbb{Z}_{p_1^m}^*$, $v \in \mathbb{Z}_{p_2}^*$. Let $\sigma_{u,v}$ be the Galois automorphism of $\mathbb{Q}(\xi_p, \xi_N)$ defined by

$\sigma_{u,v}(\xi_p) = \xi_p$, $\sigma_{u,v}(\xi_{p_1^m}) = \xi_{p_1^m}^u$, $\sigma_{u,v}(\xi_{p_2}) = \xi_{p_2}^v$. Then

$$g(\bar{\chi}_1^u \bar{\chi}_2^v) = \sigma_{u,v}(g(\bar{\chi}_1\bar{\chi}_2)) = \frac{b + c(\frac{u}{p_1})(\frac{v}{p_2})\sqrt{-p_1p_2}}{2} p^{h_0}.$$

We are now ready to compute C.

$$\begin{aligned} C &= p^{h_0} \sum_{u\in\mathbb{Z}_{p_1^m}^*} \sum_{v\in\mathbb{Z}_{p_2}^*} \left[\frac{b}{2} + \frac{c}{2}\left(\frac{u}{p_1}\right)\left(\frac{v}{p_2}\right)\sqrt{-p_1p_2}\right] \sum_{i=0}^{p_1^{m-1}-1} \chi_1^u(\gamma^{p_2 i+a})\chi_2^v(\gamma^a) \\ &= \frac{b}{2}p^{h_0}\Bigg(\sum_{i=0}^{p_1^{m-1}-1} \sum_{u\in\mathbb{Z}_{p_1^m}^*} \chi_1^u(\gamma^{p_2 i+a})\Bigg)\Bigg(\sum_{v\in\mathbb{Z}_{p_2}^*}\chi_2^v(\gamma^a)\Bigg) \\ &\quad + \frac{c}{2}p^{h_0}\sqrt{-p_1p_2}\Bigg(\sum_{i=0}^{p_1^{m-1}-1} \sum_{u\in\mathbb{Z}_{p_1^m}^*} \left(\frac{u}{p_1}\right)\chi_1^u(\gamma^{p_2 i+a})\Bigg)\Bigg(\sum_{v\in\mathbb{Z}_{p_2}^*}\left(\frac{v}{p_2}\right)\chi_2^v(\gamma^a)\Bigg) \\ &= \frac{b}{2}p^{h_0}p_1^{m-1}(p_1\delta_{j_a,p_1} - 1)(p_2\delta_{a,p_2} - 1) \\ &\quad + \frac{c}{2}p^{h_0}\sqrt{-p_1p_2}\Bigg(\sum_{i=0}^{p_1^{m-1}-1} \sum_{u\in\mathbb{Z}_{p_1^m}^*} \left(\frac{u}{p_1}\right)\chi_1^u(\gamma^{p_2 i+a})\Bigg)\Bigg(\sum_{v\in\mathbb{Z}_{p_2}^*}\left(\frac{v}{p_2}\right)\chi_2^v(\gamma^a)\Bigg). \end{aligned}$$

We have $\sum_{v\in\mathbb{Z}_{p_2}^*}\left(\frac{v}{p_2}\right)\chi_2^v(\gamma^a) = \left(\frac{a}{p_2}\right)\sqrt{p_2^*}$, where $p_2^* = (-1)^{\frac{p_2-1}{2}}p_2$, and

$$\begin{aligned} \sum_{i=0}^{p_1^{m-1}-1} \sum_{u\in\mathbb{Z}_{p_1^m}^*} \left(\frac{u}{p_1}\right)\chi_1^u(\gamma^{p_2 i+a}) &= \sum_{i=0}^{p_1^{m-1}-1}\Bigg(\sum_{u_1=1}^{p_1-1}\left(\frac{u_1}{p_1}\right)\chi_1^{u_1}(\gamma^{p_2 i+a})\Bigg)\Bigg(\sum_{u_2\in\mathbb{Z}_{p_1^{m-1}}}\chi_1^{p_1u_2}(\gamma^{p_2 i+a})\Bigg) \\ &= p_1^{m-1}\sum_{u_1=1}^{p_1-1}\left(\frac{u_1}{p_1}\right)\chi_1^{u_1}(\gamma^{p_1^{m-1}j_a}) = p_1^{m-1}\left(\frac{j_a}{p_1}\right)\sqrt{p_1^*}, \end{aligned}$$

where $p_1^* = (-1)^{\frac{p_1-1}{2}}p_1$. Therefore, putting the above computations together, we have

$$\begin{aligned} C &= \frac{b}{2}p^{h_0}p_1^{m-1}(p_1\delta_{j_a,p_1} - 1)(p_2\delta_{a,p_2} - 1) + \frac{c}{2}p^{h_0}\sqrt{-p_1p_2}\left(\frac{a}{p_2}\right)\sqrt{p_2^*}\cdot p_1^{m-1}\left(\frac{j_a}{p_1}\right)\sqrt{p_1^*} \\ &= \frac{b}{2}p^{h_0}p_1^{m-1}(p_1\delta_{j_a,p_1} - 1)(p_2\delta_{a,p_2} - 1) - \left(\frac{a}{p_2}\right)\left(\frac{j_a}{p_1}\right)\frac{c}{2}p^{h_0}p_1^m p_2 \end{aligned}$$

We conclude that

$$\begin{aligned}T_a &= p_1^{m-1}(-1+A)+B+C\\ &= -p_1^{m-1}+p_1^{m-1}(-1)^{\frac{p_1-1}{2}-1}\sqrt{q}(p_2\delta_{a,p_2}-1)+(-1)^{\frac{p_2-1}{2}-1}\sqrt{q}p_1^{m-1}(p_1\delta_{j_a,p_1}-1)\\ &\quad+\frac{b}{2}p^{h_0}p_1^{m-1}(p_1\delta_{j_a,p_1}-1)(p_2\delta_{a,p_2}-1)-\left(\frac{a}{p_2}\right)\left(\frac{j_a}{p_1}\right)\frac{c}{2}p^{h_0}p_1^m p_2\end{aligned}$$

Noting that $\{p_1 \pmod 4, p_2 \pmod 4\}=\{1,3\}$, we have

$$\begin{aligned}T_a &= -p_1^{m-1}-(-1)^{\frac{p_1-1}{2}}p_1^{m-1}p_2\sqrt{q}\delta_{a,p_2}-(-1)^{\frac{p_2-1}{2}}p_1^m\sqrt{q}\delta_{j_a,p_1}\\ &\quad+\frac{b}{2}p^{h_0}p_1^{m-1}(p_1\delta_{j_a,p_1}-1)(p_2\delta_{a,p_2}-1)-\left(\frac{a}{p_2}\right)\left(\frac{j_a}{p_1}\right)\frac{c}{2}p^{h_0}p_1^m p_2.\end{aligned}$$

We consider four cases:

(1) $\delta_{j_a,p_1}=\delta_{a,p_2}=0$. In this case, we have

$$T_a=-p_1^{m-1}+\frac{b}{2}p^{h_0}p_1^{m-1}-\left(\frac{a}{p_2}\right)\left(\frac{j_a}{p_1}\right)\frac{c}{2}p^{h_0}p_1^m p_2.$$

Set

$$\begin{aligned}c_+ &= -p_1^{m-1}+\frac{b}{2}p^{h_0}p_1^{m-1}+\frac{c}{2}p^{h_0}p_1^m p_2,\\ c_- &= -p_1^{m-1}+\frac{b}{2}p^{h_0}p_1^{m-1}-\frac{c}{2}p^{h_0}p_1^m p_2.\end{aligned}$$

Then $T_a=c_+$ or c_- according as $\left(\frac{a}{p_2}\right)\left(\frac{j_a}{p_1}\right)=-1$ or 1.

(2) $\delta_{j_a,p_1}=1,\ \delta_{a,p_2}=1$. In this case, we have

$$T_a=-p_1^{m-1}-(-1)^{\frac{p_1-1}{2}}p_1^{m-1}p_2\sqrt{q}-(-1)^{\frac{p_2-1}{2}}p_1^m\sqrt{q}+\frac{b}{2}p^{h_0}p_1^{m-1}(p_1-1)(p_2-1).$$

For future use, we will denote this value of T_a by c_1.

(3) $\delta_{j_a,p_1}=0,\ \delta_{a,p_2}=1$. In this case, we have

$$T_a=-p_1^{m-1}-(-1)^{\frac{p_1-1}{2}}p_1^{m-1}p_2\sqrt{q}-\frac{b}{2}p^{h_0}p_1^{m-1}(p_2-1).$$

For future use, we will denote this value of T_a by c_2.

(4) $\delta_{j_a,p_1}=1,\ \delta_{a,p_2}=0$. In this case, we have

$$T_a=-p_1^{m-1}-(-1)^{\frac{p_2-1}{2}}p_1^m\sqrt{q}-\frac{b}{2}p^{h_0}p_1^{m-1}(p_1-1).$$

For future use, we will denote this value of T_a by c_3.

In summary, T_a, $0\le a\le N-1$, belong to $\{c_+,c_-,c_1,c_2,c_3\}$. Therefore the restricted eigenvalues $\psi(\gamma^a D)=T_a/N$ can take at most 5 distinct values. The proof is now complete. □

We now determine when $\mathrm{Cay}(\mathbb{F}_q,D)$ is strongly regular. Recall that h is the class number of $\mathbb{Q}(\sqrt{-p_1p_2})$, and b,c appeared in (5.2).

Corollary 5.2. *Using the above notation,* $\mathrm{Cay}(\mathbb{F}_q, D)$ *is a strongly regular graph if and only if* $b, c \in \{1, -1\}$*,* h *is even and* $p_1 = 2p^{h/2} + (-1)^{\frac{p_1-1}{2}}b$*,* $p_2 = 2p^{h/2} - (-1)^{\frac{p_1-1}{2}}b$*.*

Proof: If the graph $\mathrm{Cay}(\mathbb{F}_q, D)$ is strongly regular, then by Theorem 1.1, it has precisely two distinct restricted eigenvalues. Since $c \not\equiv 0 \pmod p$, we have $c_+ \neq c_-$. Therefore we must have $c_1, c_2, c_3 \in \{c_+, c_-\}$. It follows that

$$-(-1)^{\frac{p_1-1}{2}}2p_2p^{h/2} - (-1)^{\frac{p_2-1}{2}}2p_1p^{h/2} + b(p_1p_2 - p_1 - p_2) = \epsilon_1 cp_1p_2, \quad (5.3)$$

$$-(-1)^{\frac{p_1-1}{2}}2p^{h/2} = b + \epsilon_2 cp_1, \quad (5.4)$$

$$-(-1)^{\frac{p_2-1}{2}}2p^{h/2} = b + \epsilon_3 cp_2, \quad (5.5)$$

for some $\epsilon_1, \epsilon_2, \epsilon_3 \in \{1, -1\}$. Hence h must be even. Squaring both sides of (5.4), and recall that $b^2 + p_1p_2c^2 = 4p^h$, we obtain $2b\epsilon_2 + cp_1 = cp_2$. Squaring both sides of (5.5), we obtain $2b\epsilon_3 + cp_2 = cp_1$. Combining these two equations, we have $\epsilon_3 = -\epsilon_2$. Now substracting p_2 copies of (5.4) and p_1 copies of (5.5) from (5.3), we get $b = \epsilon_1 c$. Using the same argument as in the proof of Corollary 4.2 , we deduce that $b, c \in \{1, -1\}$.

Since p_1, p_2 are positive and $b = \pm 1$, from (5.4) and (5.5) we obtain $-(-1)^{\frac{p_1-1}{2}} = \epsilon_2 c = -\epsilon_3 c$. Consequently,

$$p_1 = 2p^{h/2} + (-1)^{\frac{p_1-1}{2}}b, \quad p_2 = 2p^{h/2} - (-1)^{\frac{p_1-1}{2}}b.$$

For the converse, noting that if $b, c \in \{1, -1\}$, h is even, and $p_1 = 2p^{h/2} + (-1)^{\frac{p_1-1}{2}}b$, $p_2 = 2p^{h/2} - (-1)^{\frac{p_1-1}{2}}b$, then with $\epsilon_1 = bc$, $\epsilon_2 = -(-1)^{\frac{p_1-1}{2}}c$, $\epsilon_3 = -\epsilon_2$, the three equations, (5.3), (5.4) and (5.5), will hold. Therefore $c_1, c_2, c_3 \in \{c_+, c_-\}$. It follows that $\psi(\gamma^a D)$, $0 \leq a \leq N-1$, take precisely two distinct values $r = \frac{c_+}{N}$, $s = \frac{c_-}{N}$. Hence $\mathrm{Cay}(\mathbb{F}_q, D)$ has precisely two distinct restricted eigenvalues r and s. By Theorem 1.1, $\mathrm{Cay}(\mathbb{F}_q, D)$ is strongly regular. The proof is now complete. □

Let us find some concrete examples of srg arising in this way. Recall that the b in (5.2) is uniquely determined by the condition that $b \equiv 2p^{h/2} \pmod{\ell}$, where $\ell \in \{p_1, p_2\}$ is the prime congruent to 3 modulo 4.

Example 5.3. Let $p = 2$, $p_1 = 3$, $p_2 = 5$, $N = 3^m \cdot 5$, with $m \geq 1$. One can easily prove by induction that $f := \mathrm{ord}_N(2) = \phi(N)/2 = 4 \cdot 3^{m-1}$ for all $m \geq 1$. The class number h of $\mathbb{Q}(\sqrt{-15})$ is equal to 2 (c.f. [6, p. 514]). Since $1 + p_1p_2 = 4p^h$, we have $b, c \in \{1, -1\}$. From $b \equiv 2p^{h/2} \pmod{\ell}$, here $\ell = 3$, we get $b = 1$. The conditions in Corollary 5.2 are all satisfied. Therefore we obtain a strongly regular Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$, with

$$v = q = 2^{4 \cdot 3^{m-1}}, \ k = \frac{v-1}{15} = 16^{3^{m-1}-1} + 16^{3^{m-1}-2} + \cdots + 16 + 1,$$

and with restricted eigenvalues $r = \frac{2^{h_0+3}-1}{15}$, $s = \frac{-7 \cdot 2^{h_0}-1}{15}$, where $h_0 = \frac{f-h}{2} = 2 \cdot 3^{m-1} - 1$.

We remark that when $m = 2$, the srg in Example 5.3 is the same as Example 1.2 by De Lange.

Example 5.4. Let $p = 2$, $p_1 = 5$, $p_2 = 3$, $N = 5^m \cdot 3$, with $m \geq 1$. One can easily prove by induction that $f := \mathrm{ord}_N(2) = \phi(N)/2 = 4 \cdot 5^{m-1}$ for all $m \geq 1$. The class number h of $\mathbb{Q}(\sqrt{-15})$ is equal to 2 . Since $1+p_1p_2 = 4p^h$, we have $b, c \in \{1, -1\}$. For the same reason as in Example 5.3 we have $b = 1$. The conditions in Corollary 5.2 are all satisfied. Therefore we obtain a strongly regular Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$, with

$$v = q = 2^{4 \cdot 5^{m-1}},\ k = \frac{v-1}{15} = 16^{5^{m-1}-1} + 16^{5^{m-1}-2} + \cdots + 16 + 1,$$

and with restricted eigenvalues $r = \frac{2^{h_0+3}-1}{15}$, $s = \frac{-7 \cdot 2^{h_0}-1}{15}$, where $h_0 = \frac{f-h}{2} = 2 \cdot 5^{m-1} - 1$.

We remark that when $m = 2$, the srg in Example 5.4 is the same as Example 1.3 by Ikuta and Munemasa.

Example 5.5. Let $p = 3$, $p_1 = 5$, $p_2 = 7$, $N = 5^m \cdot 7$, with $m \geq 1$. One can easily prove by induction that $f := \mathrm{ord}_N(3) = \phi(N)/2 = 12 \cdot 5^{m-1}$ for all $m \geq 1$. The class number h of $\mathbb{Q}(\sqrt{-35})$ is equal to 2 (c.f. [6, p. 514]). Since $1 + p_1p_2 = 4p^h$, we have $b, c \in \{1, -1\}$. From $b \equiv 2p^{h/2} \pmod{\ell}$, here $\ell = 7$, we get $b = -1$. The conditions in Corollary 5.2 are all satisfied. Therefore we obtain a strongly regular Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$, with $v = q = 3^{12 \cdot 5^{m-1}}$, $k = \frac{v-1}{35}$ and with restricted eigenvalues $r = \frac{17 \cdot 3^{h_0}-1}{35}$, $s = \frac{-18 \cdot 3^{h_0}-1}{35}$, where $h_0 = \frac{f-h}{2} = 6 \cdot 5^{m-1} - 1$.

Example 5.6. Let $p = 3$, $p_1 = 7$, $p_2 = 5$, $N = 7^m \cdot 5$, with $m \geq 1$. One can easily prove by induction that $f := \mathrm{ord}_N(3) = \phi(N)/2 = 12 \cdot 7^{m-1}$ for all $m \geq 1$. The class number h of $\mathbb{Q}(\sqrt{-35})$ is equal to 2 (c.f. [6, p. 514]). Since $1 + p_1p_2 = 4p^h$, we have $b, c \in \{1, -1\}$. From the same reason as in Example 5.5 we have $b = -1$. The conditions in Corollary 5.2 are all satisfied. Therefore we obtain a strongly regular Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$, with $v = q = 3^{12 \cdot 7^{m-1}}$, $k = \frac{v-1}{35}$ and with restricted eigenvalues $r = \frac{17 \cdot 3^{h_0}-1}{35}$, $s = \frac{-18 \cdot 3^{h_0}-1}{35}$, where $h_0 = \frac{f-h}{2} = 6 \cdot 7^{m-1} - 1$.

Example 5.7. Let $p = 3$, $p_1 = 17$, $p_2 = 19$, $N = 17^m \cdot 19$, with $m \geq 1$. One can easily prove by induction that $f := \mathrm{ord}_N(3) = \phi(N)/2 = 144 \cdot 17^{m-1}$ for all $m \geq 1$. The class number h of $\mathbb{Q}(\sqrt{-323})$ is equal to 4 (c.f. [6, p. 514]). Since $1 + p_1p_2 = 4p^h$, we have $b, c \in \{1, -1\}$. From $b \equiv 2p^{h/2} \pmod{\ell}$, here $\ell = 19$, we get $b = -1$. The conditions in Corollary 5.2 are all satisfied. Therefore we obtain a strongly regular Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$, with $v = q = 3^{144 \cdot 17^{m-1}}$, $k = \frac{v-1}{323}$, and with restricted eigenvalues $r = \frac{161 \cdot 3^{h_0}-1}{323}$, $s = \frac{-162 \cdot 3^{h_0}-1}{323}$, where $h_0 = \frac{f-h}{2} = 72 \cdot 17^{m-1} - 2$.

Example 5.8. Let $p = 3$, $p_1 = 19$, $p_2 = 17$, $N = 19^m \cdot 17$, with $m \geq 1$. One can easily prove by induction that $f := \mathrm{ord}_N(3) = \phi(N)/2 = 144 \cdot 19^{m-1}$ for all $m \geq 1$. The class number h of $\mathbb{Q}(\sqrt{-323})$ is equal to 4 (c.f. [6, p. 514]). Since $1 + p_1p_2 = 4p^h$, we have $b, c \in \{1, -1\}$. For the same reason as in Example 5.7 we have $b = -1$. The conditions in Corollary 5.2 are all satisfied. Therefore we obtain a strongly regular Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$, with $v = q = 3^{144 \cdot 19^{m-1}}$, $k = \frac{v-1}{323}$, and with restricted eigenvalues $r = \frac{161 \cdot 3^{h_0} - 1}{323}$, $s = \frac{-162 \cdot 3^{h_0} - 1}{323}$, where $h_0 = \frac{f-h}{2} = 72 \cdot 19^{m-1} - 2$.

6. Concluding Remarks

We have constructed strongly regular Cayley graphs on $\mathbb{F}_q$ by using union of cyclotomic classes of $\mathbb{F}_q$ and index 2 Gauss sums. Twelve infinite families of srg with new parameters are obtained in this way. It is natural to ask whether further examples can be found by using Corollary 4.2 and 5.2. One can certainly use a computer to search for more prime pairs (p, p_1) satisfying the conditions of Corollary 4.2, and prime triples (p, p_1, p_2) satisfying the conditions of Corollary 5.2. But we suspect that it is unlikely one can find new examples in view of the computer search performed by White and Schmidt [18] and the theoretic results therein.

Another natural question is whether we get interesting fusion schemes of the cyclotomic association schemes by using the srg arising from Corollary 4.2 and 5.2. We use the construction in Section 4 to explain this problem in some detail below.

Let $q = p^f$, where p is a prime and f a positive integer. Let γ be a fixed primitive element of $\mathbb{F}_q$ and $N|(q-1)$ with $N > 1$. As usual, let $C_0 = \langle \gamma^N \rangle$, and $C_i = \gamma^i C_0$, $1 \leq i \leq N-1$, be the N-th cyclotomic classes of $\mathbb{F}_q$. Assume that $-1 \in C_0$. Define $R_0 = \{(x, x) \mid x \in \mathbb{F}_q\}$, and for $i \in \{1, 2, \ldots, N\}$, define $R_i = \{(x, y) \mid x, y \in \mathbb{F}_q, x - y \in C_{i-1}\}$. Then $(\mathbb{F}_q, \{R_i\}_{0 \leq i \leq N})$ is a symmetric association scheme, which is called *the cyclotomic association scheme of class N over $\mathbb{F}_q$*. Now assume that we are in the situation of Section 4. That is, $N = p_1^m$, where $m \geq 1$, $p_1 > 3$ is a prime such that $p_1 \equiv 3 \pmod 4$; p is a prime such that $\gcd(N, p) = 1$, and $f := \mathrm{ord}_N(p) = \phi(N)/2$. For $0 \leq k \leq p_1 - 1$, define

$$D_k = \bigcup_{i=0}^{p_1^{m-1}-1} C_{i+kp_1^{m-1}} \tag{6.1}$$

Note that D_0 is the same as D in (4.1), $D_k = \gamma^{kp_1^{m-1}} D_0$, and $D_0, D_1, \ldots, D_{p_1-1}$ form a partition of $\mathbb{F}_q^*$. Define $R'_0 = R_0$ and

$$R'_k = \{(x, y) \mid x, y \in \mathbb{F}_q, x - y \in D_{k-1}\}. \tag{6.2}$$

It is natural to ask whether $(\mathbb{F}_q, \{R'_k\}_{0 \leq k \leq p_1})$ is an association scheme. We give an affirmative answer to this question in a subsequent paper [7]. Also included in [7] are some interesting properties of this fusion scheme in relation to A.V. Ivanov's conjecture [10, 9].

References

[1] L. D. Baumert, M. H. Mills, and R. L. Ward, Uniform Cyclotomy, *J. Number Theory* **14** (1982), 67–82.

[2] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*, A Wiley-Interscience Publication, 1998.

[3] A. E. Brouwer, W. H. Haemers, *Spectra of Graphs*, course notes, available at `http://homepages.cwi.nl/~ aeb/math/ipm.pdf`

[4] A. E. Brouwer, R. M. Wilson, and Q. Xiang, Cyclotomy and strongly regular graphs, *J. Alg. Combin.* **10** (1999), 25–28.

[5] R. Calderbank, W. M. Kantor, The geometry of two-weight codes, *Bull. London Math. Soc* **18-2** (1986), 97–122.

[6] H. Cohen, *A course in computational algebraic number theory*, GTM 138, Springer, 1996.

[7] T. Feng, F. Wu, Q. Xiang, Pseudocyclic and non-amorphic fusion schemes of the cyclotomic association schemes, preprint `arXiv:1012.2181v1`.

[8] C. Godsil, Gordon Royle, *Algebraic Graph Theory*, GTM 207, Springer-Verlag, 2001.

[9] T. Ikuta, A. Munemasa, Pseudocyclic association schemes and strongly regular graphs, *Europ. J. Combin.* **31** (2010), 1513–1519.

[10] A. A. Ivanov, C. E. Praeger, Problem session at ALCOM-91, *Europ. J. Combin.* **15** (1994), 105–112.

[11] P. Langevin, Calculs de certaines sommes de Gauss, *J. Number Theory* **63** (1997), 59–64.

[12] P. Langevin, A new class of two-weight codes, in *Finite Fields and Applications* (Glasgow 1995), London Math. Soc. Lecture Note Series, No. 233, S. Cohen and H. Niederreiter, eds. Cambridge University Press, 1996, pp. 181–187.

[13] C. L. M. de Lange, Some new cyclotomic strongly regular graphs, *J. Alg. Combin.* **4** (1995), 329–330.

[14] S. L. Ma, A survey of partial difference sets, *Des. Codes Cryptogr.* **4** (1994), 221–261.

[15] O. D. Mbodj, Quadratic Gauss sums, *Finite Fields and Appl.* **4** (1998), 347–361.

[16] R. J. McEliece, Irreducible cyclic codes and Gauss sums. Combinatorics (Proc. NATO Advanced Study Inst., Breukelen, 1974), Part 1: Theory of designs, finite geometry and coding theory, pp. 179–196. Math. Centre Tracts, No. 55, Math. Centrum, Amsterdam.

[17] P. Meijer, M. van der Vlugt, The evaluation of Gauss sums for characters of 2-power order, *J Number Theory* **100** (2003), 381–395.

[18] B. Schmidt, C. White, All two-weight irreducible cyclic codes, *Finite Fields Appl.* **8** (2002), 1–17.

[19] J. Yang, L. Xia, Complete solving of explicit evaluation of Gauss sums in the index 2 case, *Sci. China Ser. A* **53** (2010), 2525–2542.

Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA. **Current Address:** Department of Mathematics, Zhejiang University, Hangzhou 310027, Zhejiang, China

E-mail address: `pku.tfeng@yahoo.com.cn`

Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA

E-mail address: `xiang@math.udel.edu`